

PAT-NO: JP02002300158A

DOCUMENT-IDENTIFIER: JP 2002300158 A

TITLE: RIGHT PROTECTION METHOD IN OVERALL DATA DISTRIBUTION  
SERVICE

PUBN-DATE: October 11, 2002

INVENTOR-INFORMATION:

NAME	COUNTRY
HARADA, HIROMI	N/A
MORI, HIROSHI	N/A
OHASHI, TETSUYA	N/A
KONISHI, KAORU	N/A
YAMAZAKI, IORI	N/A

ASSIGNEE-INFORMATION:

NAME	COUNTRY
HITACHI LTD	N/A

APPL-NO: JP2001333035

APPL-DATE: October 30, 2001

PRIORITY-DATA: 2000340395 ( November 2, 2000 ) , 2001013956 ( January 23, 2001 )

INT-CL (IPC): H04L009/32, G06F012/14 , G06K017/00

ABSTRACT:

PROBLEM TO BE SOLVED: To provide a right protection method in an overall data distribution service that uses key scrambling data to modify a master key and to produce an execution key and uses a private execution key to encrypt all data by different private execution keys even when only the master key to be managed secretly is available.

SOLUTION: The execution key is used when encryption processing is applied to various items. The mechanism for generating the execution key adopts a method where the master key on which the execution key is based and the scramble data having an optional value are scrambled by using a particular algorithm to generate the execution key. Thus, by changing the scramble data, the execution

key acting like an encryption key or a decoding key can be varied even when the master key has a fixed value. By adopting the execution key generating method for a terminal key, encryption processing can be applied to contract information by using the terminal key stored in a reception terminal for the master key and using the different execution key every time.

COPYRIGHT: (C)2002,JPO